Sub a1

CLAIMS

1. Method for issuing an electronic identity for an entity from an identity registration authority, the method comprising the steps of:

a) issuing a first electronic identity for said entity;

b) creating a request for a second electronic identity for said entity, the request including an identifier of said entity;

c) sending said request to said identity registration authority;

d) in response to said request, creating an identification response;

e) sending said identification response to said entity;

f) verifying an acceptability of said identification response by said entity;

g) in response said verifying, if said identification response is acceptable, signing digitally said identification response by said first entity;

h) sending said signed response to said identity registration authority;

i) verifying a validity of said digital signature and said identification response in said signed response; and

j) in response to said verifying, if said digital signature and identification response are valid, issuing a second identity based on said first identity.

2. The method of claim 1 further comprising a second entity by which said first entity digitally signs said identification response.

3. The method of claim 1 or 2 further comprising the steps of:

checking if the information of said second entity is available using said identifier; and

in response said checking, if said information is not available, inquiring the information of said second entity from said first entity.

4. The method of claim 2 or 3 wherein said second entity is in control of said first entity.

5. The method of claim 3 wherein said information of said second entity comprises one or more from the set containing a unique address of said second entity, the name of the holder of said second entity and previous identity or identities of said second entity.

6. The method of claim 1 further comprising the step of:

establishing and encrypting a communication channel between said first entity and said identity registration authority to ensure confidential communication there between.

7. The method of claim 1 further comprising the step of:

storing said issued second identity to the database of said identity registration authority.

8. The method of claim 1 further comprising the step of:

storing said issued second identity to the database of the issuer of said first electronic identity.

9. The method of claim 1 further comprising the step of:

combining said first and said second electronic identities to form a combined electronic identity; and

storing said combined electronic identity to the database.

10. The method of claim 1 further comprising the step of:

sending said issued second identity to said entity.

11. The method of claim 1 further comprising the step of:

sending said issued second identity to a third party.

12. The method of claim 1 before the step of issuing said second identity further comprising the steps of:

checking if additional guarantees for ensuring a validity of the first identity are to be acquired; and

in response to said checking, if additional guarantees are needed, acquiring additional guarantees.

13. The method of claim 1 further comprising the steps of:

adding a time stamp to said issued second identity; and

storing said time stamped second identity to the database of said registration authority.

14. The method of claim 1 further comprising the step of:

adding into said time stamp a expiration date of said second electronic identity.

15. The method of claim 1 further comprising the steps of:

adding a notarization to said issued second identity; and

storing said notarized second identity to the database of said registration authority.

16. The method of claim 1 further comprising the steps of:

inquiring a further identifier code to be added into said signed identification response

receiving said identifier code at said registration authority; and

verifying the validity of said identifier code at said registration authority.

17. The method of claim 16 wherein said identifier code includes one or more from the set containing biometric code of said first entity, a predetermined

character string, a fingerprint of the entity's public key, random number, certificate, and a hash code of the shared secret between said first entity and said registration authority.

18. The method of claim 1 further comprising the steps of:

creating a first hash code from said identity request at registration authority;

sending said first hash code to said second entity;

creating a second hash code from said identity request by said second entity; and

verifying a validity of said first hash code by comparing it to said second hash code before the signing of said response.

19. The method of claim 1 or 2 before the step of issuing further comprising the steps of:

sending a confirmation message to the address specified in said additional information of said entity;

receiving a confirmation response to said confirmation message at said registration authority; and

verifying the validity of said confirmation response.

20. The method of claim 19 before the step of issuing further comprising the step of:

canceling said issuing of said second electronic identity if said confirmation response is not received in a predetermined time period.

21. The method of claim 1 wherein said request for issuing said second certificate for said entity is initiated by said third party.

22. The method of claim 1 wherein said request for issuing said second certificate for said entity is initiated by said second entity.

23. The method of claim 2 wherein said request is digitally signed by said first entity before sending said request.

24. The method of claim 2 wherein said request is encrypted before sending said request.

25. The method of claim 1 further comprising the step of:

journalizing a log of all transactions during the issue process of said second electronic identity.

26. The method of claim 2 wherein said second entity is one of the following set including mobile terminal, mobile phone, personal computer, set-top box, smart card, tamper proof device, security token, software agent, pager, terminal equipment, and personal digital assistant (PDA).